

REMARKS

In the non-final Office Action, the Examiner objects to the drawings for failing to be labeled "Prior Art"; objects to the specification as failing to provide proper antecedent basis; rejects claims 6-11 under 35 U.S.C. § 112, second paragraph, as being indefinite; rejects claims 2-11 under 35 U.S.C. § 101 because the claimed recitation of a use results in an improper definition of a process; rejects claims 32 and 33 under 35 U.S.C. § 101 as directed to non-statutory subject matter; rejects claims 1, 2, 6-15, and 17-37 under 35 U.S.C. § 103(a) as unpatentable over KENT et al. (U.S. Patent Application Publication No. 2005/0036624) in view of ERIKSSON et al. (U.S. Patent No. 6,661,806); and rejects claims 3-5 and 16 under 35 U.S.C. § 103(a) as unpatentable over KENT et al. in view of ERIKSSON et al. and further in view of KIM (U.S. Patent Application Publication No. 2001/0038695). Applicant traverses these rejections.¹

By way of the present amendment, Applicant amends claims 32 and 33 to improve form. No new matter has been added by way of the present amendment. Claims 1-37 remain pending.

In accordance with Applicant's duty to provide information regarding the substance of an interview, an interview was held between Applicant's representative and Examiner La Forgia on July 31, 2007. Applicant would like to thank Examiner La Forgia for the courtesies extended during the interview. During that interview, the rejection of claims 6-11 under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite and the rejection of claims 2-11 under 35 U.S.C. § 101 due to a claimed recitation of a use that allegedly resulted in an improper definition of a process were discussed. An agreement was reached that claims 2-11 merely further define the metes and bounds of the invention and, therefore, these claims are statutory.

The drawings are objected to because Figures 1 and 2 should allegedly include "Prior Art" legends. In particular, the Examiner alleges that only that which is old is illustrated in these figures (Office Action, pg. 2). Applicant disagrees.

¹ As Applicant's remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicant's silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, motivation to combine reference, etc.) is not a concession by Applicant that such assertions are accurate or such requirements have been met, and Applicant reserves the right to analyze and dispute such assertions/requirements in the future.

Figures 1 and 2 are described on pages 7-9 of Applicant's specification, which is part of the Detailed Description section of the specification. Figure 1 illustrates an exemplary network in which Applicant's QKD (Quantum Cryptographic Key Distribution) endpoints may be implemented. Element 105 corresponds to the QKD endpoint. Figure 2 illustrates exemplary components of QKD endpoint 105. Accordingly, Applicant submits that these figures do not depict that which is old. Applicant's specification in no way discloses or suggest that these figures are prior art.

For at least these reasons, Applicant requests that the objection to the drawings be reconsidered and withdrawn.

The specification is objected to as failing to provide proper antecedent basis for claim 32. Claim 32 has been amended to recite "a computer-readable memory device." Support for this feature can be found, for example, in paragraph 30 of the specification. Therefore, withdrawal of the object to the specification is respectfully requested.

Claims 6-11 stand rejected under 35 U.S.C. § 112, second paragraph, as indefinite for not setting forth any steps involved in the method/process. Applicant respectfully traverses this rejection. Claims 6-11 further define the metes and bounds of the invention. See, for example, *In re Vamco Machine and Tool, Inc.*, 752 F.2d 1564, 1577 n.5, 224 U.S.P.Q. (BNA) 617, 625 n.5 (Fed. Cir. 1985), which held that the claims define the boundary of the invention.

For at least this reason, Applicant respectfully requests that the rejection of claims 6-11 under 35 U.S.C. § 112, second paragraph, as being indefinite be withdrawn.

Claims 2-11 stand rejected under 35 U.S.C. § 101 because the claimed recitation of a use allegedly results in an improper definition of a process. Applicant respectfully traverses this rejection. Claims 6-11 further define the metes and bounds of the invention. See, for example, *In re Vamco Machine and Tool, Inc.*, 752 F.2d 1564, 1577 n.5, 224 U.S.P.Q. (BNA) 617, 625 n.5 (Fed. Cir. 1985), which held that the claims define the boundary of the invention.

For at least this reason, Applicant respectfully requests that the rejection of claims 2-11 under 35 U.S.C. § 101 be withdrawn.

Claim 32 stands rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter for reciting a "machine-readable medium." Without acquiescing in the Examiner's rejection, but

merely to expedite prosecution, Applicant amends claim 32 to address the Examiner's concerns. As such, withdrawal of the rejection of claim 32 under 35 U.S.C. § 101 is respectfully requested.

Claim 33 stands rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter for representing software, per se. Without acquiescing in the Examiner's rejection, but merely to expedite prosecution, Applicant amends claim 33 to address the Examiner's concerns. As such, withdrawal of the rejection of claim 33 under 35 U.S.C. § 101 is respectfully requested.

Claims 1, 2, 6-15, and 17-35 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over KENT et al. in view of ERIKSSON et al. Applicant respectfully traverses this rejection.

Claim 1 recites a method of reserving a rate at which cryptographic key material is provided. The method includes sending a first reservation request for reserving a first rate from a first secret bits consuming application to a secret bits producing application; determining, by the secret bits producing application, whether the reservation request can be satisfied; and reserving the first rate for the first secret bits consuming application when the determining determines that the reservation can be satisfied. KENT et al. and ERIKSSON et al., whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, KENT et al. and ERIKSSON et al. do not disclose or suggest reserving a first rate for a first secret bits consuming application when it is determined that a reservation can be satisfied. The Examiner admits that KENT et al. does not disclose this feature and relies on column 2, lines 33-54 and 59-65 of ERIKSSON et al. as allegedly disclosing this feature (Office Action, pg. 5). Applicant respectfully disagrees with the Examiner's interpretation of ERIKSSON et al.

At column 2, lines 33-54, ERIKSSON et al. discloses:

As described herein, it is assumed that the network is able to support resource reservation from end to end. However, it will be appreciated that the invention is equally applicable when resource reservation is only available over a specific network domain, covering only a part of the end to end path. In such a case, the reservation protocol is terminated by the routers at the edges of that network domain.

Resource reservation for a user data flow may be supported by different types of reservation protocols along the end-to-end path of the flow. For example, the protocol according to an aspect of the invention may be used over a specific network domain, covering only a part of the end-to-end path. An interworking function is then needed between the network domain

supporting the protocol according to the invention and adjacent network domains using other types of reservation protocols. As a special case, an arbitrary type of reservation protocol can be used for the signalling between the user and the access node, while the network internal signalling is performed with the protocol according to the invention. The interworking function between the two types of reservation protocol is then located in the access node.

This section of ERIKSSON et al. discloses that, when resource reservation is only available over a specific network domain, the reservation protocol is terminated by the routers at the edges of that network domain. This section of ERIKSSON et al. further discloses that resource reservation for a user data flow may be supported by different types of reservation protocols along the end-to-end path of the flow. This section of ERIKSSON et al. does not mention reserving a rate for a first secret bits consuming application. Therefore, this section of ERIKSSON et al. cannot disclose or suggest reserving a first rate for a first secret bits consuming application when it is determined that a reservation can be satisfied, as required by claim 1.

At column 2, lines 59-65, ERIKSSON et al. discloses:

In accordance with preferred embodiments of the invention, the sender has a traffic contract with its network provider, under which a particular quality of service is guaranteed. This allows the network provider to offer service differentiation to users. Thus, users who are prepared to pay higher charges are able to guarantee access to higher bandwidths, or higher priority traffic handling.

This section of ERIKSSON et al. discloses that a sender has a traffic contract with its network provider, under which a particular quality of service is guaranteed. This section of ERIKSSON merely discloses that a particular quality of service is guaranteed. This section of ERIKSSON has nothing to do with reserving a first rate for a first secret bits consuming application when it is determined that a reservation can be satisfied, as required by claim 1.

For at least the foregoing reasons, Applicant submits that claim 1 is patentable over KENT et al. and ERIKSSON et al., whether taken alone or in any reasonable combination.

Claims 2, 6-15, and 17-30 depend from claim 1. Therefore, claims 2, 6-15, and 17-30 are patentable over KENT et al. and ERIKSSON et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 1.

Independent claims 31-33 recite features similar to, yet possibly of different scope than, features recited above with respect to claim 1. Therefore, claims 31-33 are patentable over KENT et al. and ERIKSSON et al, whether taken alone or in any reasonable combination, for at least reasons similar to the reasons given above with respect to claim 1.

Claim 34 recites a method of reserving a rate of providing cryptographic key material. The method includes specifying a desired consumption rate of cryptographic key material at a first network device; and reserving the desired consumption rate of cryptographic key material. KENT et al. and ERIKSSON et al. do not disclose or suggest this combination of features.

For example, KENT et al. and ERIKSSON et al. do not disclose or suggest specifying a desired consumption rate of cryptographic key material at a first network device and reserving the desired consumption rate of cryptographic key material. The Examiner admits that KENT et al. does not disclose these features and appears to rely on column 2, lines 33-54 and 59-65 of ERIKSSON et al. as allegedly disclosing this feature (Office Action, pg. 5). Applicants respectfully disagree with the Examiner's interpretation of ERIKSSON et al.

Column 2, lines 33-54 of ERIKSSON et al. has been reproduced above. This section of ERIKSSON et al. discloses that, when resource reservation is only available over a specific network domain, the reservation protocol is terminated by the routers at the edges of that network domain. This section of ERIKSSON et al. further discloses that resource reservation for a user data flow may be supported by different types of reservation protocols along the end-to-end path of the flow. This section of ERIKSSON et al. has nothing to do with specifying a desired consumption rate of cryptographic key material at a first network device and reserving the desired consumption rate of cryptographic key material, as required by claim 34.

Column 2, lines 59-65 of ERIKSSON et al. has been reproduced above. This section of ERIKSSON et al. discloses that a sender has a traffic contract with its network provider, under which a particular quality of service is guaranteed. This section of ERIKSSON merely discloses that a particular quality of service is guaranteed. This section of ERIKSSON has nothing to do with specifying a desired consumption rate of cryptographic key material at a first network device and reserving the desired consumption rate of cryptographic key material, as required by claim 34.

If this rejection is maintained, Applicant respectfully requests that the Examiner point out how the above sections of ERIKSSON et al. can reasonably be construed as disclosing the features of claim 34.

For at least the foregoing reasons, Applicant submits that claim 34 is patentable over KENT et al. and ERIKSSON et al., whether taken alone or in any reasonable combination.

Claim 35 recites a method of reserving a rate of providing secret bits by a secret bit producer that is based on advantage distillation. The method includes specifying a desired rate by a first process; and reserving the desired rate by the secret bit producer that is based on advantage distillation. KENT et al. and ERIKSSON et al., whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, KENT et al. and ERIKSSON et al. do not disclose or suggest reserving a desired rate by a secret bit producer that is based on advantage distillation. The Examiner admits that KENT et al. does not disclose this feature and relies on column 2, lines 33-54 and 59-65 of ERIKSSON et al. as allegedly disclosing this feature (Office Action, pg. 10). Applicant respectfully disagrees with the Examiner's interpretation of ERIKSSON et al.

Column 2, lines 33-54 of ERIKSSON et al. has been reproduced above. This section of ERIKSSON et al. discloses that, when resource reservation is only available over a specific network domain, the reservation protocol is terminated by the routers at the edges of that network domain. This section of ERIKSSON et al. further discloses that resource reservation for a user data flow may be supported by different types of reservation protocols along the end-to-end path of the flow. This section of ERIKSSON et al. has nothing to do with reserving a desired rate by a secret bit producer that is based on advantage distillation, as required by claim 35.

Column 2, lines 59-65 of ERIKSSON et al. has been reproduced above. This section of ERIKSSON et al. discloses that a sender has a traffic contract with its network provider, under which a particular quality of service is guaranteed. This section of ERIKSSON merely discloses that a particular quality of service is guaranteed. This section of ERIKSSON et al. has nothing to do with reserving a desired rate by a secret bit producer that is based on advantage distillation, as required by claim 35.

If this rejection is maintained, Applicant respectfully requests that the Examiner point out how the above sections of ERIKSSON et al. can reasonably be construed as disclosing the above feature of claim 35.

For at least the foregoing reasons, Applicant submits that claim 35 is patentable over KENT et al. and ERIKSSON et al., whether taken alone or in any reasonable combination.

Claim 36 recites a method of reserving a rate of providing generated cryptographic key material from an advantage distillation based on secret bits producer. The method includes generating, by the advantage distillation based secret bits producer, cryptographic key material; receiving a request from a secure communication process for a reservation of the cryptographic key material at a first rate, the request identifying a minimum acceptable rate; and notifying the secure communication process of a successful reservation when an available generated rate of cryptographic key material is greater than the minimum acceptable rate. KENT et al. and ERIKSSON et al., whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, KENT et al. and ERIKSSON et al. do not disclose or suggest notifying a secure communication process of a successful reservation when an available generated rate of cryptographic key material is greater than a minimum acceptable rate. The Examiner admits that KENT et al. does not disclose this feature and relies on column 2, lines 33-54 and 59-65 of ERIKSSON et al. as allegedly disclosing this feature (Office Action, pg. 10). Applicant respectfully disagrees with the Examiner's interpretation of ERIKSSON et al.

Column 2, lines 33-54 of ERIKSSON et al. has been reproduced above. This section of ERIKSSON et al. discloses that, when resource reservation is only available over a specific network domain, the reservation protocol is terminated by the routers at the edges of that network domain. This section of ERIKSSON et al. further discloses that resource reservation for a user data flow may be supported by different types of reservation protocols along the end-to-end path of the flow. This section of ERIKSSON et al. has nothing to do with notifying a secure communication process of a successful reservation when an available generated rate of cryptographic key material is greater than a minimum acceptable rate, as required by claim 36.

Column 2, lines 59-65 of ERIKSSON et al. has been reproduced above. This section of ERIKSSON et al. discloses that a sender has a traffic contract with its network provider, under which a particular quality of service is guaranteed. This section of ERIKSSON merely discloses that a particular quality of service is guaranteed. This section of ERIKSSON et al. has nothing to do with notifying a secure communication process of a successful reservation when an available generated rate of cryptographic key material is greater than a minimum acceptable rate, as required by claim 36.

If this rejection is maintained, Applicant respectfully requests that the Examiner point out how the above sections of ERIKSSON et al. can reasonably be construed as disclosing the above feature of claim 36.

For at least the foregoing reasons, Applicant submits that claim 36 is patentable over KENT et al. and ERIKSSON et al., whether taken alone or in any reasonable combination.

Claim 37 recites a method of reserving a rate of providing secret key material for protecting communications. The method includes specifying a minimum desired consumption rate of secret key material and a priority by a client process; determining, by a secret key material producing process, whether the minimum desired consumption rate of secret key material is available to the client process; when the minimum desired consumption rate of secret key material is not available to the client process, making at least the minimum desired consumption rate of secret key material available by canceling at least one previously made reservation of a rate of the secret key material, each of the at least one previously made reservation having a lower priority than the specified priority; and reserving at least the minimum desired consumption rate of the secret key material for the client process. KENT et al. and ERIKSSON et al., whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, KENT et al. and ERIKSSON et al. do not disclose or suggest determining whether a minimum desired consumption rate of secret key material is available to a client process. The Examiner admits that KENT et al. does not disclose this feature and relies on column 2, lines 33-54 and 59-65 of ERIKSSON et al. as allegedly disclosing this feature (Office Action, pg. 12). Applicant respectfully disagrees with the Examiner's interpretation of ERIKSSON et al.

Column 2, lines 33-54 of ERIKSSON et al. has been reproduced above. This section of ERIKSSON et al. discloses that, when resource reservation is only available over a specific network domain, the reservation protocol is terminated by the routers at the edges of that network domain. This section of ERIKSSON et al. further discloses that resource reservation for a user data flow may be supported by different types of reservation protocols along the end-to-end path of the flow. This section of ERIKSSON et al. has nothing to do with determining whether a minimum desired consumption rate of secret key material is available to a client process, as required by claim 37.

Column 2, lines 59-65 of ERIKSSON et al. has been reproduced above. This section of ERIKSSON et al. discloses that a sender has a traffic contract with its network provider, under which a particular quality of service is guaranteed. This section of ERIKSSON merely discloses that a particular quality of service is guaranteed. This section of ERIKSSON et al. has nothing to do with determining whether a minimum desired consumption rate of secret key material is available to a client process, as required by claim 37.

If this rejection is maintained, Applicant respectfully requests that the Examiner point out how the above sections of ERIKSSON et al. can reasonably be construed as disclosing the above feature of claim 37.

For at least the foregoing reasons, Applicant submits that claim 37 is patentable over KENT et al. and ERIKSSON et al., whether taken alone or in any reasonable combination.

Claims 3-5 and 16 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over KENT et al. in view of ERIKSSON et al. and KIM. Applicant respectfully traverses this rejection.

Claims 3-5 and 16 depend from claim 1. The disclosure of KIM does not remedy the deficiencies in the disclosures of KENT et al. and ERIKSSON et al. set forth above with respect to claim 1. Therefore, claims 3-5 and 16 are patentable over KENT et al., ERIKSSON et al., and KIM, whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 1.

In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration and allowance of pending claims 1-37.

If the Examiner believes that the application is not now in condition for allowance, Applicant respectfully requests that the Examiner contact the undersigned to discuss any outstanding issues.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 18-1945, under Order No. BBNT-P01-265 from which the undersigned is authorized to draw.

Dated: August 7, 2007

Respectfully submitted,

By 

Edward A. Gordon

Registration No.: 54,130

FISH & NEAVE IP GROUP, ROPES & GRAY
LLP

One International Place

Boston, Massachusetts 02110

(617) 951-7000

(617) 951-7050 (Fax)

Attorneys/Agents For Applicant